Notice of Allowability	Application No.	Applicant(s)	
	09/940,026	LEE ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment received on 01/18/2007*.

2. ☒ The allowed claim(s) is/are *1,2,5,8-14,16-18 and 20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *03/28/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jonathan W. Hallman (Reg. No. 42,622) on March 29, 2007.

The application has been amended as follows:

Amendment to the Specification

Please replace the paragraph beginning on page 1, line 7 with the following replacement paragraph:

This application is related to U.S. Patent Application ~~Serial~~ No. 09/542,510, "Digital Rights Management within an Embedded Storage Device" to Lane W. Lee and Daniel R. Zaharris, now U.S. Pat. No. 6,636,966 ~~Attorney Docket No. M-8382 US~~, filed April 3, 2000, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 1, line 11 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/940,083 [[_____]], "A Secure Access Method and System" to Timothy R. Feldman, Lane W. Lee, Michael F. Braitberg, Douglas M. Rayburn, and Gary G. Kiwimagi, now U.S. Pat. No. 7,110,982 ~~Attorney Docket No. M-9793 US~~, filed herewith, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 1, line 15 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/940,174 [[_____]], "System and Method for Detecting Unauthorized Copying of Encrypted Data" to Lane W. Lee, Timothy R. Feldman, Douglas M. Rayburn, and Gary G. Kiwimagi, ~~Attorney Docket No. M-12038 US,~~ filed herewith, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 1, line 19 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/940,025 [[_____]], "System and Method for Identifying Vendors of Hidden Content" to Steven B. Volk, Michael F. Braitberg, Timothy R. Feldman, Lane W. Lee, Douglas M. Rayburn, and Gary G. Kiwimagi, now abandoned ~~Attorney Docket No. M-12039 US~~, filed herewith, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 1, line 24 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/940,035 [[_____]], "An Unlocking Method and System for Data on Media" to Lane W. Lee, Timothy R. Feldman, Douglas M. Rayburn, and Gary G. Kiwimagi, ~~Attorney Docket No. M-12040 US,~~ filed herewith, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 2, line 1 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/939,896 [[_____]], "A Revocation System and Apparatus for Secure Content" to Lane W. Lee, Timothy R. Feldman, Douglas M. Rayburn, and Gary G. Kiwimagi, ~~Attorney Docket No. M-12042 US,~~ filed herewith, which application is incorporated herein for all purposes.

Please replace the paragraph beginning on page 2, line 5 with the following replacement paragraph:

This application is related to U.S. Patent Application No. 09/939,960 [[_____]], "A Mastering Process and System for Secure Content" to Lane W. Lee, Timothy R. Feldman, Douglas M. Rayburn, and Gary G. Kiwimagi, now abandoned ~~Attorney Docket No. M-12043 US~~, filed herewith, which application is incorporated herein for all purposes.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (currently amended): A method of authenticating a host to receive content from a media player, the method comprising:

receiving at the media player a certificate from the host, the certificate including a plurality of fields, including a field holding a digital signature from a certifying authority, the certificate also including data, wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the host;

verifying the digital signatures in the certificate, the verifying including at least one of:

verifying the certifying authority digital signature using the certifying authority public key; and

verifying a host digital signature using a host public key;

receiving validation data from a source~~, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria~~;

comparing the data in the certificate to the validation data from the source to identify as valid or invalid one or more of the product category, the product line, the model, the revision and the serial number of the host;

if the digital signatures are verified and the validation data is validated, generating a random number at the media player to form a session key and encrypting the session key with a

public key extracted from the certificate to form an encrypted session key and transmitting the encrypted session key to the host;

at the host, decrypting the encrypted session key using a host private key to recover the session key;

at the media player, encrypting a content key using the session key to provide an encrypted content key;

at the host, receiving an encrypted content key from the media player;

decrypting the encrypted content key using the session key to recover the content key;

at the media player, retrieving encrypted content from a media;

transmitting the encrypted content to the host; and

at the host, decrypting the encrypted content using the content key.

2. (Original) The method of claim 1 wherein the source is one of a portable medium and firmware.

3. (Cancelled)

4. (Cancelled)

5. (Previously Presented) The method of claim 1 wherein the certifying of the host includes certifying a second host for a host to second host secure communication channel, the certifying allowing a copy function between the host and the second host.

6. (cancelled)

7. (cancelled)

8. (Previously Presented) The method of claim 1 wherein the certificate includes one or more of a certifying authority identifier field, a version field, a sign key identifier field, an exposed methods field, a company field, a model identifier field, a revision field, a metadata identifier field, a device digital signature key field, a certifying authority digital signature field, a serial number field, a protocol public key field and a device digital signature field, wherein the certifying authority digital signature verifies one or more of the fields in the certificate and the host digital signature verifies one or more of the fields in the certificate.

9. (Previously Presented) The method of claim 1 wherein the certificate enables an entity receiving the certificate to control the quality of the host by invalidating hosts that are false or have latent defects.

10. (currently amended): The method of claim 1 ~~6~~ wherein the certificate further includes fields provided by a host manufacturer, including the company public key, wherein the company public key is digitally signed by the certifying authority.

11. (currently amended): The method of claim 1 ~~6~~ wherein the certificate further includes fields provided by a host manufacturer, the fields including the host public key, wherein the host public key is digitally signed by the company.

12. (currently amended) The method of claim 1 ~~6~~ wherein one or more of the product category, the product line, the model, the revision and the serial number of the host are provided to a certificate creator after the host passes a qualification procedure.

13. (Original) The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key.

14. (Previously Presented) The method of claim 13 wherein the set of methods includes digital rights management (DRM) methods include one or more of a copy method, a record method, a play method, a read secure metadata method, a write secure metadata method, and an unlock method, the DRM methods operable according to a type of the host.

15. (Cancelled)

16. (Original) The method of claim 1 wherein each of the fields hold 326-bit values for 163-bit elliptic curve cryptography.

17. (Original) The method of claim 1 wherein the certifying authority public key is referenced by a field of the certificate.

18. (previously presented) The method of claim 1 wherein the certifying authority public key is in a firmware component.

19. (Cancelled)

Claim 20(currently amended): A media player configured to certify a host, the media player comprising:

a firmware component including:

a block configured to receive a certificate from the host, the certificate including a plurality of fields, including a field holding a protocol public key, the certificate also including data, wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the host;

a block configured to verify one or more digital signatures in the certificate, including at least one of:

a certifying authority digital signature using a certifying authority public key; and

a device digital signature using a device public key in the certificate;

a block configured to receive validation data from a source, the validation data identifying one or more of the product category, the product line, the model, the revision and the serial number of the host data in the certificate as valid or invalid according to predetermined criteria;

a block configured to generate a random number and transmit the random number to the host if the digital signatures are verified and the validation data is validated; and

a block configured to encrypt a content key using the random number to provide an encrypted content key and to transmit ~~an~~ the encrypted content key to the host, wherein the host is enabled to recover a content key from the encrypted content key by using the random number, the media player being operable to retrieve encrypted content from a media and provide the encrypted content to the host such that the host is enabled to decrypt the encrypted content using the content key.

Claims 21-23. (cancelled)

REASONS FOR ALLOWANCE

1. Claims 1-2, 5, 8-14, 16-18, and 20 are allowed.

2. The following is an examiner's statement of reasons for allowance:

3. The above-mentioned claims are allowable over the Cited Prior Art (CPA) of record, because the CPA of record fails to teach or render obvious the claimed limitations as recited in currently amended independent claims 1 and 20, and subsequent dependent claims.

4. The CPA fails to teach a media player, or a method of authenticating a host to the media player which comprises receiving at the media player a certificate from the host, wherein the certificate includes validation data including one or more of a product category, a product line, a model, a revision and a serial number of the host, whereby the validation information is validated at the media player, and if it is found that the validation data is valid and the digital signatures are correct, a random number (session key) is created at the media player and sent to the host for decrypting the encrypted content key used to decrypt the content sent from the media player to the host.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA 03/29/07
KA
03/29/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100